ABSTRACT OF THE DISCLOSURE

Mechanism are provided for a trusted intermediary partner to mange the encryption/decryption keys of trading partners in a trading community. As the trusted intermediary manages the public signature decryption keys for each potential sender, the recipient does not have to manage these keys. In one embodiment, a recipient receives a message from a sender via the trusted intermediary, knowing that the message originates from an authentic sender, but not from an imposter. The sender sends the message together with a digital signature of the sender, which is created from the private signature creation key of the sender, to the trusted intermediary. The trusted intermediary, having the public signature decryption key associated with the private signature creation key of the sender, uses this public signature decryption key to authenticate the sender, i.e., verifying that the message originates from a real sender, and not an imposter. Upon verifying that the message indeed originates from the authentic sender, the trusted intermediary sends the message together with a digital signature of the trusted intermediary, which is created from the private signature creation key of the trusted intermediary, to the recipient. The recipient, receiving the message and the digital signature and having the public signature decryption key associated with the private signature creation key of the trusted intermediary, uses this public signature decryption key to authenticate the trusted intermediary, i.e., verifying that the message comes from an authentic trusted intermediary, and not an imposter. If the message indeed comes from the authentic trusted intermediary, then the recipient knows that the message originates from the authentic sender, who has been authenticated by the trusted intermediary. In one embodiment, the trading partners may use message encryption/decryption keys to encrypt/decrypt the message. In this embodiment, the trusted intermediary maintains public message encryption keys of all potential recipients, eliminating the need for each sender to manage these public message encryption keys.